EXHIBIT 6

CIS Benchmarks

CIS Apple iOS 13 and iPadOS 13 Benchmark

v1.0.0 - 11-12-2019

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

Table of Contents

Overview

This document, *Security Configuration Benchmark for Apple iOS 13 and iPadOS 13*, provides prescriptive guidance for establishing a secure configuration posture for the Apple iOS and iPadOS version 13. This guide was tested against the Apple iOS 13.2 and iPadOS 13.2 and using Apple Configurator v2.11.1. This benchmark covers the Apple iOS 13 and iPadOS 13 on all supported devices. As of the publication of this guidance, devices supported by iOS 13 or iPadOS 13 include the following:
• iPhone 6s and later • iPod touch (7th generation) and later • iPad Pro and later • iPad (5th generation) • iPad Air 2 • iPad mini 4 and later
In determining recommendations, the current guidance consider iOS and iPadOS devices as having the same use cases and risk/threat scenarios. In all but a very few cases, configuration steps, default settings, and benchmark recommended settings are identical regardless of hardware platform or operating system; for the few cases where variation exists, the benchmark notes the difference within the respective section. To obtain the latest version of this guide, please visit http://cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at *support@cisecurity.org*.

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, end users, and platform deployment personnel who plan to use, develop, deploy, assess, or secure solutions that incorporate the Apple iOS 13 or iPadOS 13.

Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been published. During this phase, all feedback provided by the

Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus process, please visit https://workbench.cisecurity.org/.

3.2.1.4 (L1) Ensure 'Allow iCloud backup' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to allowing iCloud backup.

Rationale:

iCloud backups are encrypted in transit and at rest within Apple's infrastructure, but there is no protection against restoring a backup to an unmanaged device. This allows for data leakage.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, that the checkbox for `Allow iCloud backup` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `iCloud backup not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Allow iCloud backup`.
5. Deploy the Configuration Profile.

CIS Controls:

Version 6

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

Version 7

13.4 Only Allow Access to Authorized Cloud Storage or Email Providers
Only allow access to authorized cloud storage or email providers.

3.2.1.5 (L1) Ensure 'Allow iCloud documents & data' is set to 'Disabled' (Scored)

Profile Applicability:

- Level 1 - Institutionally Owned Devices

Description:

This recommendation pertains to the storage and sync of data through iCloud from institutionally owned devices.

Rationale:

Institutionally owned devices are often connected to personal iCloud accounts. This is expected and normal. The data from institutionally owned devices though should not co-mingle with the end-user's personal data. This poses a potential avenue of data leakage.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, verify that under the tab `Functionality`, that the checkbox for `Allow iCloud documents & data` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Profile`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Documents in the Cloud not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Restrictions` tab.
4. In the right windowpane, under the tab `Functionality`, `uncheck` the checkbox for `Allow iCloud documents & data`.

5. Deploy the Configuration Profile.

CIS Controls:

Version 6

14 Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

Version 7

13.4 Only Allow Access to Authorized Cloud Storage or Email Providers
Only allow access to authorized cloud storage or email providers.